Spam Scams:
How to protect yourself

What is spam?

Also known as unsolicited commercial e-mail (UCE), spam consists of e-mail messages sent in bulk without prior request or consent. Low in cost and often untraceable, spam promotes get-rich-quick scams and other misleading schemes. Typically, e-mail solicitors or spammers obtain e-mail addresses by buying lists from brokers who harvest addresses from Internet newsgroup postings, chat rooms, Web sites and other online services' membership directories. The spammers then use special software to send thousands, and in some cases millions of e-mail messages to potential victims.

How to protect yourself from spam

If you're tempted to respond to a spam that is likely a scam, the FTC and the Office of the Indiana Attorney General suggests you stop and ask yourself two important questions:
1. Why would a perfect stranger pick you to share a fortune with?
2. Why would you share your personal or business information, including your bank account numbers or your company letterhead, with someone you don't know?

To avoid spam and other forms of unwanted solicitation, please review the following hints:

• Be cautious about opening any attachment or downloading any files from e-mails.
• Avoid e-mailing personal or financial information.
• Try not to display your e-mail address in public.
• Contact the company or agency cited in an e-mail to confirm legitimacy.
• If you get an e-mail or pop-up message that asks for personal or financial information, do not reply or click the link in the message.
• Read and understand the entire form before you transmit personal information through a Web site.
• Remind yourself to ignore the promises of strangers.
• Check the privacy policy when you submit your address to a Web site.
• Use anti-virus software and a firewall, and keep them up to date.
• Forward spam that is "phishing" for information to spam@uce.gov.
• Decide if you want to use two e-mail addresses: one for personal messages and the other for newsgroups and chat rooms.
• Use a unique e-mail address that utilizes both letters and numbers to decrease spam.
• Use an e-mail filter.
• Complain to the sender's Internet service provider. Most ISPs have rules against using the system to SPAM others.
• Report spam to the FTC.
• Let the FTC know if a "remove me" request is not honored.

Be aware of typical scams

Phishing: A high-tech scam designed to obtain people's financial information, "phishing" uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords and other sensitive information. E-mail messages asking you to update, validate or confirm account information are widespread, and some even threaten consequences if you don't respond.
The Nigerian Scam: FTC informants have reported receiving numerous offers from supposed Nigerian officials who promise big profits in exchange for help moving large sums of money out of their country. According to the FTC, these "officials" offer to transfer millions of dollars into your bank account in change for a small fee.

Vacation Prize Promotions: Electronic certificates congratulating you on "winning" a fabulous vacation for a very attractive price are another common scam. Often, the cruise ship and hotel accommodations are shabby, and you may be required to pay more for
an upgrade.

Credit Repair: Credit repair scams offer to erase accurate negative information from your credit file so you can qualify for a credit card, auto loan, home mortgage or a job. However, only time, a deliberate effort and a personal debt repayment plan will improve your credit. Remember, if you lie on an application for a loan, job or credit card, you will be committing fraud.

Business Opportunities: These scams promise a lot of income without much work or cash outlay. The solicitations trumpet unbelievable earnings and claim that the business doesn't involve selling, meetings or personal contact with others. These scams are usually illegal pyramid schemes masquerading as legitimate opportunities to earn money.

Bulk E-mail: Bulk e-mail solicitations offer to sell you lists of e-mail addresses so you can send your own bulk solicitations. However, sending bulk e-mail violates the terms of service of most Internet service providers. Several states have laws regulating the sending of unsolicited commercial e-mail, which you may unwittingly violate by sending bulk e-mail.

Chain Letters: You're asked to send a small amount of money—usually between $5 and $20—to each of four or five names on a list, replace one of the names on the list with your own, and then forward the revised message via bulk e-mail. Chain letters are almost always illegal, and nearly all of the people who participate in them lose their money.

Work-At-Homes Schemes: Envelope-stuffing solicitations promise steady income for minimal labor. Commonly, you'll pay a small fee to get started, then, you'll learn that the e-mail sender never had real employment to offer. Instead, you'll get instructions on how to send the same envelope-stuffing ad in your own bulk e-mailings. If you earn any money, it will be from others who fall for the same scheme.

Health and Diet Scams: Pills promising you'll lose weight without exercising or changing your diet and cures for common health problems are among the scams flooding e-mail boxes. Beware of testimonials from "cured" consumers or "famous" medical experts. These ads usually use phrases like "scientific breakthrough," "miraculous cure," "exclusive product," "secret formula" or "ancient ingredient."

Effortless Income or Investment: The trendiest get-rich-quick schemes offer unlimited profits exchanging money on world currency markets; newsletters describing a variety of easy-money opportunities; the perfect sales letter; and the secret to making $4,000 in one day. The thought of easy money may be appealing, but success generally requires hard work. Investment schemes promise outrageously high rates of return with no risk. Promoters of fraudulent investments often close down before they can be detected and reopen under another name, to sell another investment scam.

Free Goods: Some e-mail messages offer valuable goods, like cell phones, TVs and computers, at no cost to you. You're asked to pay a fee to join a club and then told that to earn the offered goods, you have to bring in a certain number of participants. Most of these messages are pyramid schemes that inevitably collapse. Some e-mail messages offer home-equity loans that don't require equity in your home, regardless of your credit history. Usually, the home equity loans turn out to be useless lists of lenders who will turn you down if you don't meet their qualifications

Resources

The Consumer Protection Division of the Indiana Attorney General's Office works to safeguard the rights of Indiana citizens every day. If you have questions or complaints regarding spam scams, or other appropriate consumer issues, contact the Attorney General's Consumer Protection Division using the web address and phone number listed below.

Office of the Indiana Attorney General
Consumer Protection Divison

To file a complaint call 1.800.382.5516
or visit www.IndianaConsumer.com